ISO/TS 23535:2022-01 (E)

Health informatics - Requirements for customer-oriented health cloud service agreements

Contents

Page

Foreword ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 Cloud computing in health and healthcare **4**
4.1 Cloud computing in hospital 4
4.2 Gap between CSC's expectation and CSP's solution 4

5 CSA for health and healthcare **5**
5.1 Roles and responsibilities 5
5.1.1 Cloud service customer 5
5.1.2 Cloud service provider 7
5.2 Service support 12
5.2.1 Service catalogue 12
5.2.2 Service coverage 13
5.2.3 Uninterrupted service 13
5.2.4 Accountability for service interruption 13
5.2.5 Compensation for service interruption 13
5.2.6 Service downtime 13
5.2.7 Service disruption notification 13
5.2.8 Target response time 14
5.2.9 Information on subcontractors 14
5.3 Service model 14
5.4 Service monitoring 14
5.5 Incident reporting 15
5.5.1 Incident report 15
5.5.2 Incident response 15
5.5.3 Incident report delivery 15
5.5.4 Repair time 15
5.6 Standards, testing, and certification 15
5.6.1 Conformity with international standards 15
5.6.2 Guidelines for ensuring compatibility between clouds 15
5.6.3 Support data input 16
5.6.4 Adopt international standards 16
5.6.5 Compliance with non-international standards 16
5.6.6 Compliance test 16
5.6.7 Compliance with updated standards 16
5.6.8 Certification details 16
5.7 Data location 16
5.7.1 Cloud service area and location 16
5.7.2 Cloud relocation 16
5.7.3 Violation of advance notice 16
5.8 Data governance 16
5.8.1 Cloud data maintenance policy 16
5.8.2 Cloud data backup plan 17
5.8.3 Cloud data collection 17
5.8.4 Cloud data query history 17
5.9 Data security 17

5.9.1 Technical security measures 17
5.9.2 Administrative security measures 17
5.9.3 Physical security measures 18
5.9.4 Simulation for technical security measures 18
5.9.5 Data integrity assurance 18
5.9.6 De-identification 18
5.10 Data transfer 18
5.10.1 Data transfer deadline 18
5.10.2 Data transfer method 18
5.10.3 Data transfer roles 18
5.10.4 Data deletion method 18
5.10.5 Data transfer customer approval 18
5.10.6 Approved data transfer range 18
5.10.7 Responsibilities for data transfer violation 19
5.11 Billing system and operation policies 19
5.11.1 Billing system criteria 19
5.11.2 Internal cloud operational policy 19
5.11.3 Billing for excess usage 19
5.12 Payments 19
5.12.1 Payment method/time 19
5.12.2 Payment period 19
5.12.3 Payment method 19
5.12.4 Explanation of billing details 19
5.13 Regulatory compliance 19
5.13.1 Jurisdiction compliance 19
5.14 Service update and version management 20
5.14.1 Service update notification 20
5.14.2 Change notification upon service update 20
5.14.3 Service update stability assessment 20
5.14.4 Service version management 20
5.15 Agreement renewal and expiry 20
Annex A (informative) **Summary of security and privacy and metric model components** **21**
Annex B (informative) **Service catalogues and cost estimate** **23**
Bibliography **26**